2

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-312593
(43)Date of publication of application : 28.11.1995

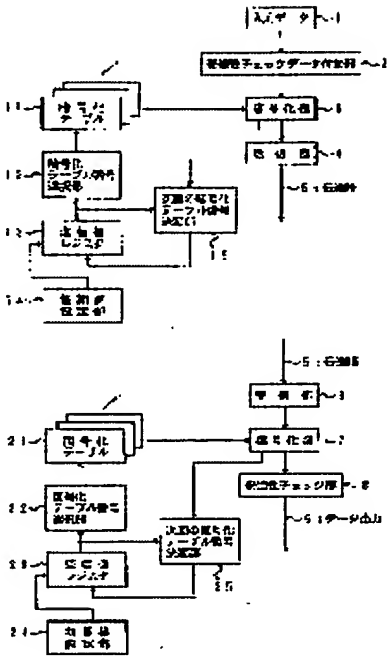
(51)Int.Cl. H04L 9/06
H04L 9/14
G09C 1/00

(21)Application number : 06-125923
(22)Date of filing : 17.05.1994

(71)Applicant : NEC CORP
(72)Inventor : INOUE TAKAHIRO

(54) ON-LINE TELEGRAPH ENCODING DEVICE

(57)Abstract:
PURPOSE: To improve the secret effect by deciding an encoding table number as the output and the function of a telegraph number and deciding the code table number by a decoding table number decision part.
CONSTITUTION: In an input data 1, the data proper to check the propriety of decoding in a propriety check data addition part 2 is added. The selected encoding table 11 encodes it in an encoding part 3, then it is sent to a transmission line 5. When encoding is ended, the next encoding table number decision part 15 decides the encoding table number to be used the next time and sets it in a transmission register 13. A reception part 6 accepts the data from the transmission line 5, and it is decoded in a decoding part 7 with the decoding table 21 of the selected number. A propriety check part 8 checks the proper decoding of the added data in the addition part 2 and outputs it. A next decoding table number decision part 25 decides the number of the decoding table to be used next and sets it in a reception register 23.



LEGAL STATUS

[Date of request for examination] 17.05.1994
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 2595899
[Date of registration] 09.01.1997
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－312593

(43)公開日　平成７年(1995)11月28日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/06				
	9/14				
Ｇ０９Ｃ	1/00		9364－5L		
				Ｈ０４Ｌ　9/02　Ｚ	

審査請求　有　請求項の数４　ＦＤ　（全　５　頁）

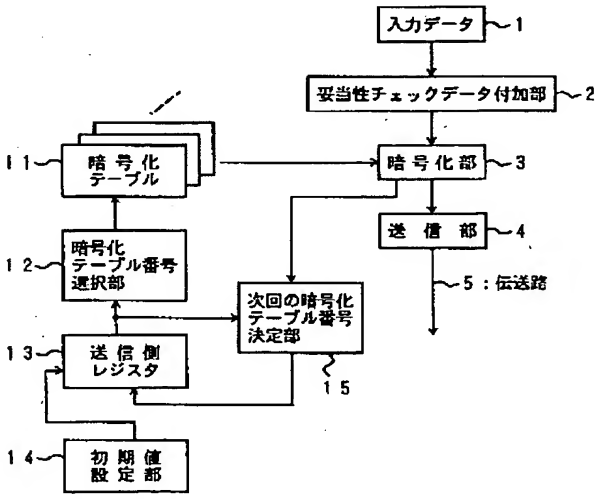
(21)出願番号　特願平6－125923

(22)出願日　平成６年(1994)５月17日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　井上　貴博
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　弁理士　高橋　友二

(54)【発明の名称】　オンライン伝文暗号化装置

(57)【要約】
【目的】　暗号化データの解読を一層困難にする。
【構成】　送信側と受信側とで同じ関数を使用して現在使用中の暗号（復号）化テーブル番号から次回使用するテーブル番号を算出する。



1

【特許請求の範囲】

【請求項１】　送信側に設けられる複数種類の暗号化テーブル、

この複数種類の暗号化テーブルの各テーブルを区別するテーブル番号を付し何番の暗号化テーブルを使用するかを決定する暗号化テーブル番号選択部、

この暗号化テーブル番号選択部が選択すべき番号数が登録されている送信側レジスタ、

この送信側レジスタに登録されている数値を初期化する初期値設定部、

暗号化して送信すべきデータを前記暗号化テーブル番号選択部で選択した暗号化テーブルによって暗号化する暗号化部、

前記暗号化して送信すべきデータの暗号化が前記暗号化部において終了した時点で前記送信側レジスタの出力数値の関数として次回の暗号化に使用する暗号化テーブルの番号を決定する次回の暗号化テーブル番号決定部、

この次回の暗号化テーブル番号決定部で決定した暗号化テーブル番号を前記送信側レジスタに登録する手段、

前記暗号化部で暗号化したデータを伝送路に送出する送信部、

受信側に設けられる複数種類の復号化テーブルであって、各復号化テーブルは送信側の各暗号化テーブルによって暗号化されたデータを復号するためのテーブルとして作成され対応する暗号化テーブルと同一のテーブル番号が付された複数種類の復号化テーブル、

この複数種類の復号化テーブルの何番の復号化テーブルを使用するかを決定する復号化テーブル番号選択部、

この復号化テーブル番号選択部が選択すべき番号数が登録されている受信側レジスタ、

この受信側レジスタに登録されている数値を初期化する初期値設定部、

前記伝送路を経て伝送されたデータを受信する受信部、

この受信部で受信したデータを前記復号化テーブル番号選択部で選択した復号化テーブルによって復号する復号化部、

前記受信したデータの復号が前記復号化部において終了した時点で前記受信側レジスタの出力数値の前記関数として次回の復号に使用する復号化テーブルの番号を決定する次回の復号化テーブル番号決定部、

この次回の復号化テーブル番号決定部で決定した復号化テーブル番号を前記受信側レジスタに登録する手段、

を備えたオンライン伝文暗号化装置。

【請求項２】　前記次回の暗号化テーブル番号決定部は、前記送信側レジスタの出力数値をアドレスとし、そのアドレス位置に次回に使用すべき暗号化テーブル番号が記憶されるＲＯＭを備え、前記次回の復号化テーブル番号決定部は、前記受信側レジスタの出力数値をアドレスとし、そのアドレスに次回に使用すべき復号化テーブル番号が記憶されるＲＯＭを備えたことを特徴とする請求項第１項記載のオンライン伝文暗号化装置。

2

【請求項３】　前記次回の暗号化テーブル番号決定部は、前記送信側レジスタの出力数値及び当該伝文に付けられた伝文番号の関数として次回の暗号化に使用する暗号化テーブル番号を決定し、次回の復号化テーブル番号決定部は、前記受信側レジスタの出力数値及び当該伝文に付けられた伝文番号の前記関数として次回の暗号化に使用する暗号化テーブル番号を決定することを特徴とする請求項第１項記載のオンライン伝文暗号化装置。

【請求項４】　前記暗号化して送信すべきデータには、所定のビットパターンを有する妥当性チェックデータが付加されており、前記復号化部で復号したデータのうちの妥当性チェックデータの部分が前記所定のビットパターンに復号されるか否かをチェックする妥当性チェック部が設けられることを特徴とする請求項第１項～第３項記載のオンライン伝文暗号化装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、データ伝送に際し、伝送路上で傍受されることを避けるためのオンライン伝文暗号化装置に関するものである。

【０００２】

【従来の技術】従来のこの種の暗号化装置としては、送信側に１種類の暗号化テーブル（ここでいう暗号化テーブルは、全ての暗号化手段を代表していう）を持ち、受信側ではその暗号化テーブルで暗号化した暗号を復号する復号化テーブル（同様に全ての復号化手段を代表していう）を持っているシステムがある。このようなシステムでは、暗号化テーブルが固定しているため、伝送路上である期間傍受されると暗号化データが解読され易くなるという危険がある。

【０００３】この危険を軽減するため、送信側に複数種類の暗号化テーブルを持ち、受信側では各暗号化テーブルに対応する復号化テーブルを持ち、送信側ではどの暗号化テーブルを使ったかという情報を伝文に入れて送信し、受信側では送信側で使用した暗号化テーブルに対応する復号化テーブルを使用している。然しながら、どの暗号化テーブルを使用したかという情報を伝送路上に送出することは、それだけ暗号化データを解読し易くするという危険がある。また、どの暗号化テーブルを使用したかという情報（これを暗号化鍵ということにする）が雑音などによる障害により正確に伝送できない場合があるので、暗号化鍵が正確に伝送されたかどうかを受信側で確認しなければならない

【０００４】特開平２－１８０４４６号公報（以下、先行技術１という）で「暗号化鍵配送確認方式」と題して開示された方式では、送信側には暗号化のマスタキーを備え、受信側にはこれに対応する復号化のマスタキーを備え、暗号化鍵は第１回目は暗号化マスタキーにより暗号化して送信し、受信側では復号化マスタキーでこれを

復号して送信側が送出した暗号化鍵を復号し、以後はこの暗号化鍵に対応する復号化鍵で復号するように接続を変更しておく。

【０００５】送信側では、第２回目には送出すべき暗号化鍵を当該暗号化鍵によって暗号化して送出する。受信側ではこれを受信し当該暗号化鍵に対応する復号化鍵で復号するので、第１回目と同様な復号結果が得られる筈である。もしそうでなければ、どこかにエラーがあったとして再送を要求する。

【０００６】

【発明が解決しようとする課題】以上のような従来の装置では、文献１に開示された方法では、複数の暗号化テーブルを備えて随時選択した暗号化テーブルを使用し、且つどの暗号化テーブルを使用するかという情報、すなわち暗号化鍵を暗号化して受信側へ送出するので、暗号を傍受解読されるという危険性を低減させることはできるが、暗号化鍵の送出とその確認の操作が大変煩わしい操作を要求されるという問題点があった。

【０００７】本発明は従来のものにおける上述の問題点を解決するためになされたもので、暗号化鍵の送出確認を行うことなく、送信側の暗号化テーブルの番号変更に対応して受信側の復号化テーブルの番号を自動的に変更し、送信側の暗号化と受信側の復号とを整合することができるオンライン伝文暗号化装置を提供することを目的としている。

【０００８】

【課題を解決するための手段】本発明では現在使用している暗号化（復号化）テーブルの番号をｘとするとき次に使用する暗号化（復号化）テーブルの番号ｚは、ｚ＝ｆ（ｘ）で示されるｘの関数として算出することとし、この関数ｆ（ｘ）は送信側と受信側とで同一関数を使用することにより暗号化鍵を暗号化して送出する必要をなくし、暗号化テーブル番号と復号化テーブル番号とを整合することとした。

【０００９】すなわち、本発明のオンライン伝文暗号化装置は、送信側に設けられる複数種類の暗号化テーブル、この複数種類の暗号化テーブルの各テーブルを区別するテーブル番号を付し何番の暗号化テーブルを使用するかを決定する暗号化テーブル番号選択部、この暗号化テーブル番号選択部が選択すべき番号数が登録されている送信側レジスタ、この送信側レジスタに登録されている数値を初期化する初期値設定部、暗号化して送信すべきデータを前記暗号化テーブル番号選択部で選択した暗号化テーブルによって暗号化する暗号化部、前記暗号化して送信すべきデータの暗号化が前記暗号化部において終了した時点で前記送信側レジスタの出力数値の関数として次回の暗号化に使用する暗号化テーブルの番号を決定する次回の暗号化テーブル番号決定部、この次回の暗号化テーブル番号決定部で決定した暗号化テーブル番号を前記送信側レジスタに登録する手段、前記暗号化部で

暗号化したデータを伝送路に送出する送信部、受信側に設けられる複数種類の復号化テーブルであって、各復号化テーブルは送信側の各暗号化テーブルによって暗号化されたデータを復号するためのテーブルとして作成され対応する暗号化テーブルと同一のテーブル番号が付された複数種類の復号化テーブル、この複数種類の復号化テーブルの何番の復号化テーブルを使用するかを決定する復号化テーブル番号選択部、この復号化テーブル番号選択部が選択すべき番号数が登録されている受信側レジスタ、この受信側レジスタに登録されている数値を初期化する初期値設定部、前記伝送路を経て伝送されたデータを受信する受信部、この受信部で受信したデータを前記復号化テーブル番号選択部で選択した復号化テーブルによって復号する復号化部、前記受信したデータの復号が前記復号化部において終了した時点で前記受信側レジスタの出力数値の前記関数として次回の復号に使用する復号化テーブルの番号を決定する次回の復号化テーブル番号決定部、この次回の復号化テーブル番号決定部で決定した復号化テーブル番号を前記受信側レジスタに登録する手段を備えたことを特徴とする。

【００１０】また、前記次回の暗号化テーブル番号決定部は、前記送信側レジスタの出力数値をアドレスとし、そのアドレス位置に次回に使用すべき暗号化テーブル番号が記憶されるＲＯＭを備え、前記次回の復号化テーブル番号決定部は、前記受信側レジスタの出力数値をアドレスとし、そのアドレスに次回に使用すべき復号化テーブル番号が記憶されるＲＯＭを備えたことを特徴とする。

【００１１】また、前記次回の暗号化テーブル番号決定部は、前記送信側レジスタの出力数値及び当該伝文に付けられた伝文番号の関数として次回の暗号化に使用する暗号化テーブル番号を決定し、次回の復号化テーブル番号決定部は、前記受信側レジスタの出力数値及び当該伝文に付けられた伝文番号の前記関数として次回の暗号化に使用する暗号化テーブル番号を決定することを特徴とする。

【００１２】さらに、前記暗号化して送信すべきデータには、所定のビットパターンを有する妥当性チェックデータが付加されており、前記復号化部で復号したデータのうちの妥当性チェックデータの部分が前記所定のビットパターンに復号されるか否かをチェックする妥当性チェック部が設けられることを特徴とする。

【００１３】

【実施例】以下、本発明の実施例を図面について説明する。図１は本発明の一実施例の送信側装置を示すブロック図、図２は受信側装置を示すブロック図である。複数の暗号化テーブル１１の各テーブルに対応して、それぞれ復号化テーブル２１が設けられる。暗号化テーブル１１と復号化テーブル２１とには、それぞれ番号が付けられており暗号化の際に使用した暗号化テーブル１１と同

じ番号の復号化テーブル２１を使用すると正しく複合できるように構成される。

【００１４】使用する暗号化テーブルの番号は、暗号化テーブル番号選択部１２で選択され、暗号化テーブル番号選択部１２は、送信側レジスタ１３に設定されている数値の番号の暗号化テーブル１１を選択する。一方、使用する復号化テーブルの番号は、復号化テーブル番号選択部２２で選択され、復号化テーブル番号選択部２２は受信側レジスタ２３に設定されている数値の番号の復号化テーブル２１を選択する。

【００１５】入力データ１には、妥当性チェックデータ付加部２で復号の妥当性をチェックするに適したデータが付加され、選択された暗号化テーブルで暗号化部３において暗号化されて送信部４から伝送路５へ送出される。暗号化部３における暗号化が終了すると、次回の暗号化テーブル番号決定部１５は次回使用する暗号テーブルの番号を決定し、送信側レジスタ１３にセットする。送信側レジスタ１３の初期値は、初期値設定部１４で設定される。

【００１６】受信部６は伝送路からのデータを受信し、選択された番号の復号化テーブルを用いて復号化部７で復号し、妥当性チェックデータ付加部２で付加されたデータが正しく復号されていることを、妥当性チェック部８でチェックした上で、データ出力９として出力する。復号化部７における復号が終了すると、次回の復号化テーブル番号決定部２５は次回使用する復号化テーブルの番号を決定し、受信側レジスタ２３にセットする。受信側レジスタ２３の初期値は、初期値設定部２４で設定される。

【００１７】次回の暗号化テーブル番号決定部１５と次回の復号化テーブル番号決定部２５とは、現在使用中のテーブル番号ｘから、同一の関数ｚ＝ｆ（ｘ）を使用して次回のテーブル番号ｚを決定する。例えば、１０種類のテーブルがあり、第０～９番の番号が付けてあり、ｚ＝ｆ（ｘ）は簡単にｚ＝ｘ＋３（但し、この加法はモジュロ１０（テーブルの種類数）の加法である）とすれば、最初に送信側レジスタ１３も受信側レジスタ２３も数値０に初期化されていると、両レジスタの数値は０から出発して、０，３，６，９，２，５，８，１，４，７，０のように一巡して変化し、暗号化テーブル１１と復号化テーブル２１とは、常に同一の番号のものが選ばれ、暗号化データは正しく復号される。

【００１８】次回の暗号（復号）化テーブル番号決定部１５（２５）の動作を、一層複雑にすることも可能である。例えば、送出する文書に数値ｙを入れて送り、ｚ＝ｇ（ｘ，ｙ）の関数としてｚを決定することとすれば良い。図３は、このような構成の次回の暗号（復号）化テーブル番号決定部１５（２５）の構成例を示し、ＲＯＭ３０にはＸアドレスがｘでＹアドレスがｙの位置に、ｚ＝ｇ（ｘ，ｙ）のｚの値が記憶されていて、Ｘアドレスデコーダ３１にｘの値を、Ｙアドレスデコーダ３２にｙの値を入力すれば、ｚの値を読み出すことができる。ｚ＝ｆ（ｘ）の関数に対してもＲＯＭを使用できることは言うまでもない。

【００１９】以上のように本発明では、暗号化テーブルに対応する復号化テーブルを正確に自動的に選択することができ、その妥当性をもチェックすることができる。但し、この妥当性チェックは、本発明の必須条件ではない。

【００２０】

【発明の効果】以上説明したように本発明によれば、使用する暗号化テーブルをその都度変更することができ、且つ、変更した旨の情報を伝送路上に送出する必要もないので、操作が容易で秘匿効果をさらに向上させることができる等の効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例の送信側の構成を示すブロック図である。

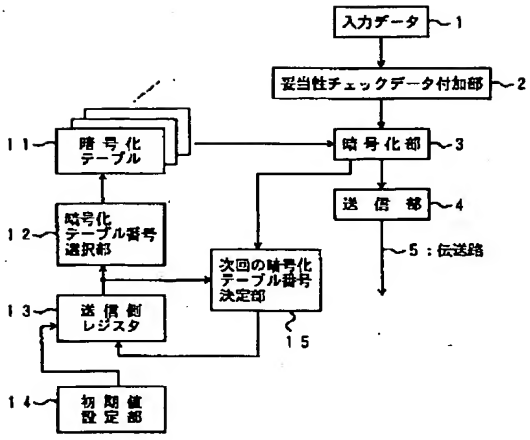
【図２】本発明の一実施例の受信側の構成を示すブロック図である。

【図３】図１に示す次回の暗号化テーブル番号決定部の構成例を示すブロック図である。

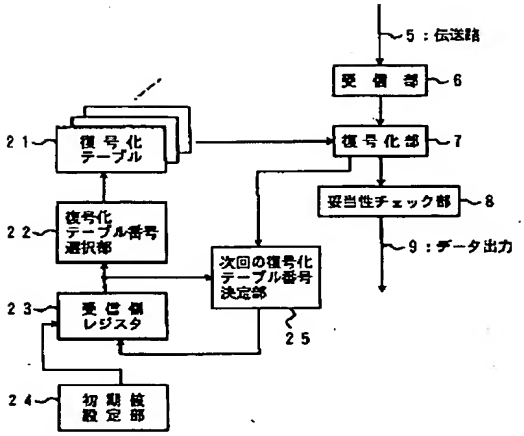
【符号の説明】

１　入力データ
２　妥当性チェックデータ付加部
３　暗号化部
４　送信部
５　伝送路
６　受信部
７　復号化部
８　妥当性チェック部
１１　暗号化テーブル
１２　暗号化テーブル番号選択部
１３　送信側レジスタ
１４　初期値設定部
１５　次回の暗号化テーブル番号決定部
２１　復号化テーブル
２２　復号化テーブル番号選択部
２３　受信側レジスタ
２４　初期値設定部
２５　次回の復号化テーブル番号決定部

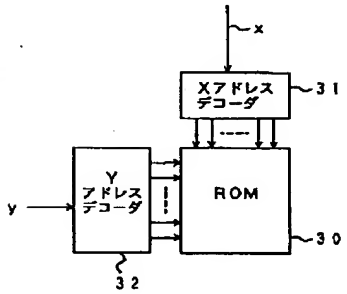
【図１】


入力データ
1
妥当性チェックデータ付加部
2
暗号化テーブル
11
暗号化部
3
送信部
4
5：伝送路
暗号化テーブル番号選択部
12
次回の暗号化テーブル番号決定部
15
送信側レジスタ
13
初期値設定部
14

【図２】


5：伝送路
受信部
6
復号化テーブル
21
復号化部
7
妥当性チェック部
8
9：データ出力
復号化テーブル番号選択部
22
次回の復号化テーブル番号決定部
25
受信側レジスタ
23
初期値設定部
24

【図３】


x
Xアドレスデコーダ
31
Yアドレスデコーダ
y
ROM
30
32